Domain Squatting:

There Is Always Someone Waiting for Your Typos

DuskRise

Imagine this: Soon it will be your kid's birthday and you have just found the perfect present for a worthwhile price on Amazon. You know it would make them happy. You decide to buy it, so you add it to the cart, fill in your credit card details, click "confirm", and yes! You got it! Your kid will be happy to receive that present.

Something is off though.

You read the URL twice to be sure:

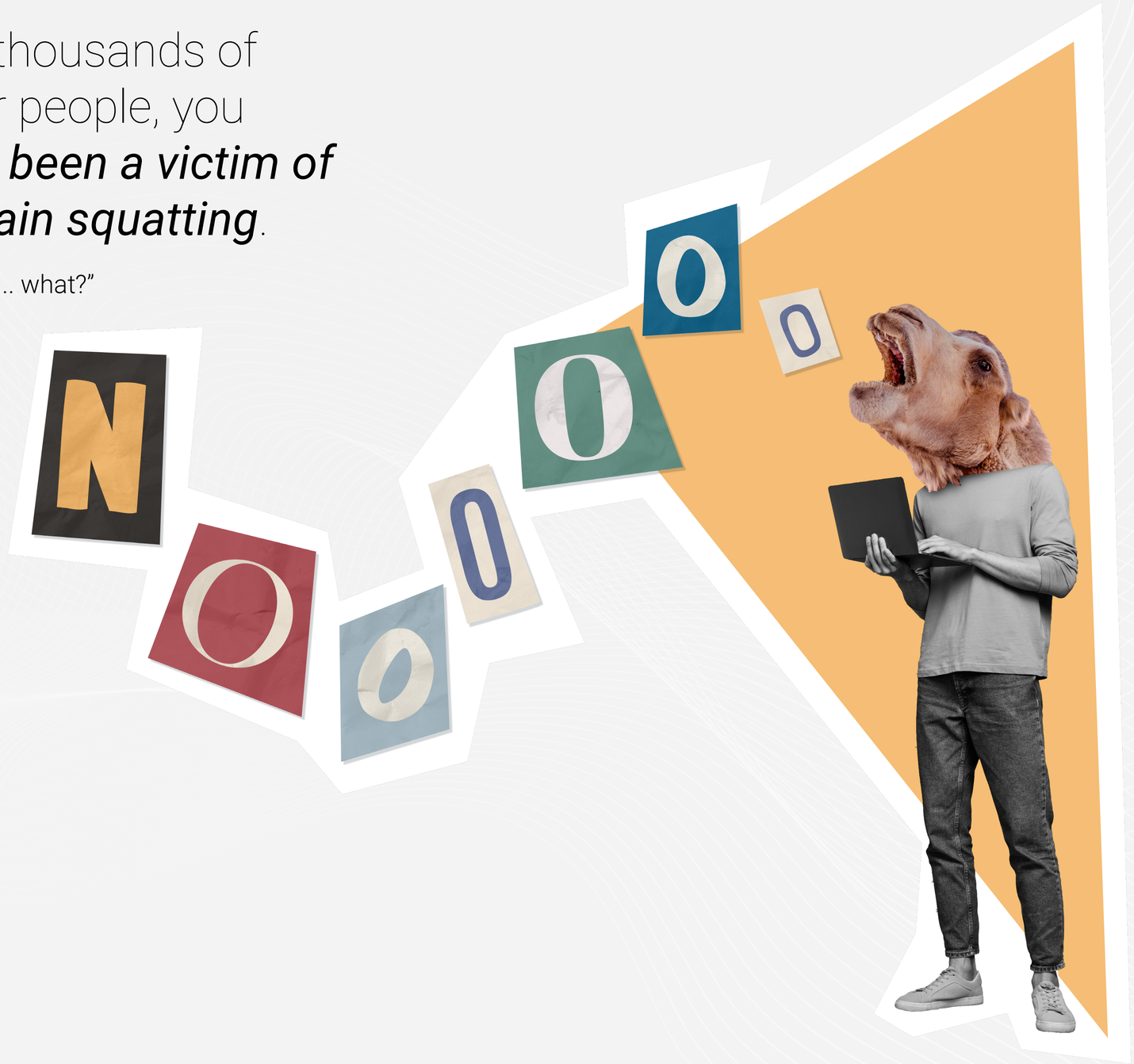
"amaz… n.com?
Where is the O?"

You have just realized you weren't on "amazon[.]com" as you intended, but on "`amazn[.]com`".

The website looks unsuspiciously identical to the original, but **your credit card number and security code** are now stored on a server that knows where and owned by who knows who.

Like thousands of other people, you ***have been a victim of domain squatting***.

"Domain… what?"



Domain Squatting 101

Domain squatting (a.k.a. cybersquatting) is the practice of registering or buying a domain name with the intent of profiting from the reputation of someone else's brand/trademark.

Cybercriminals can lead unsuspecting internet users to **alternative websites which resemble a well-known or established brand/trademark**, either by registering domain names confusingly similar to the original, as in our previous scenario, or luring them to fall victim to a phishing or smishing campaign.

The **"typos"** that can doom you could be several. From the example above we know that removing characters is an option.

But hackers can indeed leverage a wide variety of ***typosquatting techniques***:

Character swapping

when two consecutive characters belonging to a trademark or brand are swapped
e.g., `wahtsapp`

Key proximity

when a character is replaced with another character located in a keyboard position close to the former
e.g., `alliahz`

Numeric substitution

e.g., `g00gle`

Top Level Domain (TLD) squatting

when the attacker registers the brand domain with a different TLD
e.g. `twitter[.]info` instead of `twitter[.]com`

Combosquatting

when an extra word is added separated with a '-'
e.g., `paypal-usd`

Character insertion/deletion

e.g., `tpaypal`, `crdit-agricole`

Why Is Domain Squatting a Thing?

Cybercriminals can ***monetize*** domain squatting actions in several profitable ways.

First of all, by **exploiting disclosed information**. After falling victim to domain squatting, users may be redirected to a website that looks identical to the legitimate site.
Once on the fake website, they might be prompted to enter personal information such as login credentials, credit card numbers, or other sensitive data. This information can then be used by attackers for a variety of malicious purposes, such as **identity theft**, **financial fraud**, or other types of cybercrime.

Another way is **selling registered domains** to companies that want to protect their customers and their brand.

Since registering a domain is cheap for most TLDs and a domain can be sold for a lot of money to the victim company, this blackmail-like opportunity makes domain squatting very profitable.

Additionally, as registrants may not have any fake content to point the domains to, they can leverage advertisements provided by some services to also **monetize users' traffic flow.**

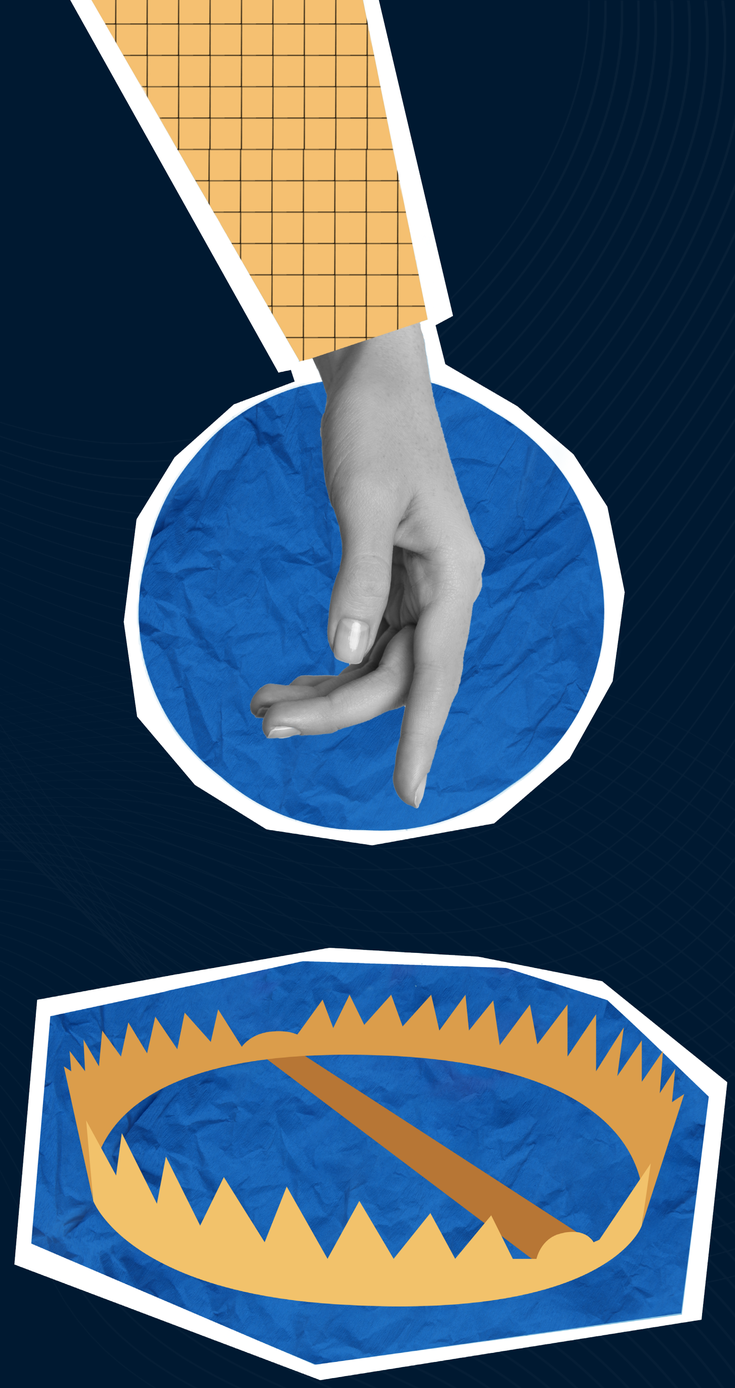
This method is called **"domain parking"**, and it's not illegal per se but it might become harmful in case, for example, a parked domain serves malicious ads.
In this scenario, the registrant gets a fee every time a user clicks on an ad that is linked to another malicious website or a drive-by download attack; once the malware is installed, it can be used to steal sensitive data, monitor the victim's online activity, or even take control of their device.

How Do I Avoid Falling into the Trap?

Since making mistakes is something we cannot really avoid (we're humans, right?) there are a few tips one can follow to minimize the possibility of falling victim to domain squatting:

- When googling to find a website, **check carefully** that you are about to open the correct one;
- When googling to find a website, try **avoiding the sponsored ones**, since they could be malicious;
- **Bookmark** the websites you often use so you don't have to type them;
- **Double-check the spelling** of URLs before entering any personal information;
- Download software or other files only from **trusted sources**;
- **Deploy security software** such as browser/ad protection tools, anti-virus, and anti-malware programs as it can help to mitigate the risk of falling victim to typosquatting or other types of cyber attacks.

It is worth noting that not only companies but ***also celebrities can fall victim to domain squatting***. It happened to the singer Madonna, who won the case against a cybersquatter who allocated a porn site under the madonna[.]com domain.



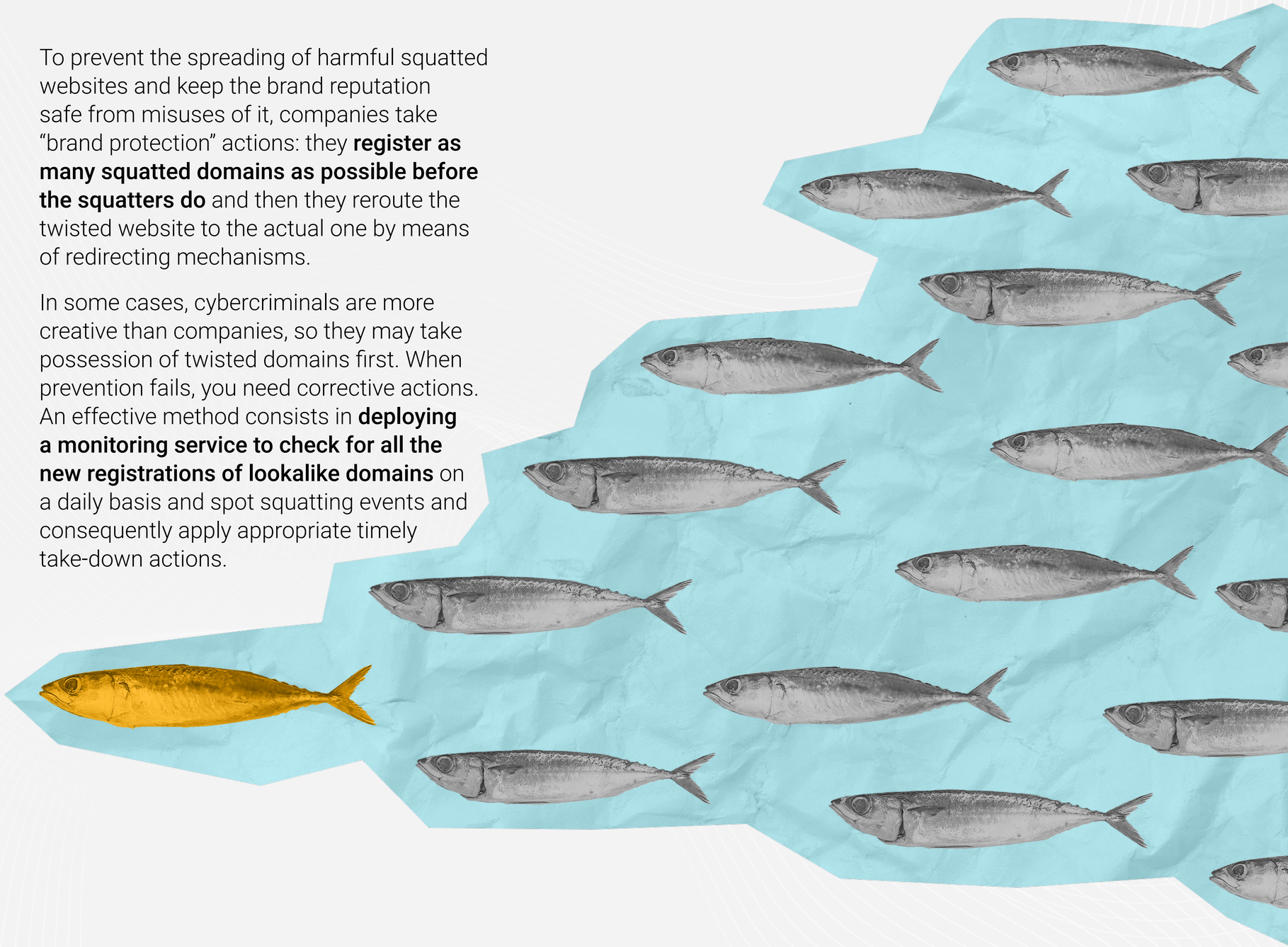
The Importance of Brand Protection

Our recent studies revealed that the most squatted brands belong to e-commerce, search engines, technology, and social media industries. Brands like Google, Amazon, Facebook, iPhone, and Microsoft are being squatted constantly. To give some figures:

Each brand is squatted with an average of ***15 twisted domain registrations per day***, which makes ***5500ish a year each***.

To prevent the spreading of harmful squatted websites and keep the brand reputation safe from misuses of it, companies take "brand protection" actions: they **register as many squatted domains as possible before the squatters do** and then they reroute the twisted website to the actual one by means of redirecting mechanisms.

In some cases, cybercriminals are more creative than companies, so they may take possession of twisted domains first. When prevention fails, you need corrective actions. An effective method consists in **deploying a monitoring service to check for all the new registrations of lookalike domains** on a daily basis and spot squatting events and consequently apply appropriate timely take-down actions.



How We Tackle Domain Squatting at DuskRise

DuskRise has developed its own proprietary pipeline for detecting potential squatted domains. The process is fully automated, and it is inspired by state-of-art techniques.

It mostly goes around these steps:

- **Collection;**
- **Processing;**
- **Monitoring;**
- *Repeat.*

Collection

We keep an eye on **newly registered domains** by ingesting and filtering them every day from different sources to store them in our database systems.
We use fancy tools to make sure our information is **correct and always up-to-date**.

Processing

We then put every single new domain through a wide range of algorithms to detect all of the **typosquatting techniques** mentioned above and more, to then store them and evaluate them alongside domain-related **contextual data (metadata)**, which allows us to find infrastructure information related to the potential squatting case.

Monitoring

Tracking a squat domain is not a once-in-a-lifetime process. Whenever we detect a potentially squatted domain, we need to **continuously analyze** that domain and keep it monitored **to be aware of any changes** that may arise, like if it became active and when, by also analyzing its metadata and other useful information. This also allows us to find common behavior and patterns among squatting domains and **act as quickly as possible** if any take-down action needs to be done.

Just by looking at some of the ***registered domain names*** we collect on a daily basis, we could find a bunch of ***potential squatting cases***. To mention a few:

```
amazon198[.]com
your-account-amazon-verify[.]com
amaz0n[.]asia
micrcosoft[.]info
fasebook[.]org
api-drive-google[.]com
googgle[.]me
microsoftdefenders[.]com
```

All of these examples were detected as soon as they were registered and thus, before they became active. Moreover, we're able to identify the registrar and hosting services to make the first approach to the squatter, if needed. Furthermore, we were also able to detect that, once these sites became active, they were blocked by some security vendors.

Use Case: Financial Analyst Scams

This technology is particularly effective when it comes to preventing and taking down squatted domains. Let's see a practical example of how we leveraged it to spot abuses out in the wild.

Recently, our team was asked to analyze some suspicious activity happening in the world of financial services.

Spoiler alert!

We were able to identify a network of fraudulent activities:
the attack was transversal as it did not target any specific financial firm, but rather involved several US firms.

The journey starts by leveraging a broker database to collect a bunch of domains regarding financial advisors and firms, to then apply our set of procedures to spot suspicious cases and after correlate them with other metadata to detect several **mismatches between the actual entity and the scam**, like gender discrepancy, syntax errors on the website narrative, etc., and discovered not only the attack network but also the patterns in the infrastructure used by the fraudulent actors, such as IP addresses, ASNs, and so on.

Take care!

If you are a business, taking all the necessary steps to build up a robust preventive and reactive posture to handle such an attack is crucial and when ignored can lead to a loss of reputation and money. Monitor your domains frequently and consult an expert to help you avoid falling victim to this practice! By doing so, you can **protect your brand's reputation** and avoid any negative consequences that may arise from domain squatting.

If you are a customer instead, don't forget to follow our suggestions. At DuskRise everyone wants to make sure you get to give the birthday present to your kid.

Domain squatting is a serious issue that can be dangerous both for businesses and customers.

Based both in the European Union and the United States and powered by its internal unit Cluster25, DuskRise deploys its Cyber Threat Intelligence solution globally, providing organizations with nation-state caliber threat intelligence and expert guidance.

Cluster25 experts are specialized in global threat hunting and adversary hunting practices. They independently design and develop technologies aimed at the classification and categorization of malicious artifacts as well as for their correlation with known threat groups.

Relying on extensive visibility into the digital threat landscape, we overcome the usual limitations of services based on ex-post threat observation by providing real predictive and proactive intelligence services.

DISCOVER MORE